UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,508	06/29/2001	James S. Magdych	NAI1P011/01.116.01	7235

28875 7590 12/09/2004

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/895,508	MAGDYCH ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 June 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 110 (page 6, line 20). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: figure 1, reference character 408. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not

to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 12-22 and 26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 12 and 26 state "a computer program product of", a computer program product is considered non-statutory subject matter. Dependent claims 13-22 are rejected based on their dependency from claim 12.

To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1-3, 5-7, 9-10, 12-14, 16-18, 20-21, 23-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Shostack et al.

Regarding claim 1, Shostack et al. teach a method of remotely detecting vulnerabilities on a local computer, comprising: installing an agent on a local computer (column 4, lines 32-46, column 11, lines 40-60); receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 8, lines 19-31); decrypting the commands on the local computer utilizing the agent (column 10, lines 10-41); processing the commands on the local computer utilizing the agent (column 10, lines 10-41); and performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 3, lines 15-20).

Regarding claim 2, Shostack et al. teach the method as recited in claim 1, wherein the agent includes a plurality of risk-assessment modules (column 2, lines 61-67, column 3, lines 1-37).

Regarding claim 3, Shostack et al. teach the method as recited in claim 2, wherein the commands execute the risk- assessment modules in a specific manner that is configured at the remote computer (column 12, lines 7-9).

Regarding claim 5, Shostack et al. teach the method as recited in claim 2, wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a

given function, a GETPWENT module for retrieving an entry from a password database, a GETORENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command (column 3, lines 6-37, column 7, lines 20-30, column 12, lines 27-40, column 13, lines 18-30).

Regarding claim 6, Shostack et al. teach the method as recited in claim 2, wherein the risk-assessment modules are selected from the group consisting of a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command (column 3, lines 6-37, column 7, lines 20-30, column 12, lines 14-40, column 13, lines 18-30).

Regarding claim 7, Shostack et al. teach the method as recited in claim 1, wherein the commands each indicate at least one of the risk-assessment modules (column 12, lines 14-26).

Regarding claim 9, Shostack et al. teach the method as recited in claim 1, and further comprising transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network (column 13, lines 24-25 and 37-44).

Regarding claim 10, Shostack et al. teach the method as recited in claim 9, and further comprising receiving feedback to the results from the remote computer utilizing the network (column 13, lines 24-25 and 37-44).

Regarding claim 12, Shostack et al. teach a computer program product of remotely detecting vulnerabilities on a local computer, comprising: computer code for installing an agent on a local computer (column 4, lines 32-46, column 11, lines 40-60); computer code for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 8, lines 19-31); computer code for decrypting the commands on the local computer utilizing the agent (column 10, lines 10-41); computer code for processing the commands on the local computer utilizing the agent (column 10, lines 10-41); and computer code for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 3, lines 15-20).

Regarding claim 13, Shostack et al. teach the computer program product as recited in claim 12, wherein the agent includes a plurality of risk-assessment modules (column 2, lines 61-67, column 3, lines 1-37).

Regarding claim 14, Shostack et al. teach the computer program product as recited in claim 13, wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer (column 12, lines 7-9).

Regarding claim 16, Shostack et al. teach the computer program product as recited in claim 13, wherein the risk- assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR

module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command (column 3, lines 6-37, column 7, lines 20-30, column 12, lines 27-40, column 13, lines 18-30).

Regarding claim 17, Shostack et al. teach the computer program product as recited in claim 13, wherein the risk- assessment modules are selected from the group consisting of a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM module for performing a checksum operation on a file, and an EXEC module for executing a command (column 3, lines 6-37, column 7, lines 20-30, column 12, lines 14-40, column 13, lines 18-30).

Regarding claim 18, Shostack et al. teach the computer program product as recited in claim 12, wherein the commands each indicate at least one of the risk-assessment modules (column 12, lines 14-26).

Regarding claim 20, Shostack et al. teach the computer program product as recited in claim 12, and further comprising computer code for transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network (column 13, lines 24-25 and 37-44).

Regarding claim 21, Shostack et al. teach the computer program product as recited in claim 20, and further comprising computer code for receiving feedback to the results from the remote computer utilizing the network (column 13, lines 24-25 and 37-44).

Regarding claim 23, Shostack et al. teach a system of remotely detecting vulnerabilities on a local computer, comprising: acn agent installed on a local computer (column 4, lines 32-46, column 11, lines 40-60) for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 8, lines 19-31), decrypting the commands on the local computer (column 10, lines 10-41), and processing the commands on the local computer (column 10, lines 10-41); and wherein the risk-assessment scan is performed on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 3, lines 15-20).

Regarding claim 24, Shostack et al. teach a system of remotely detecting vulnerabilities on a local computer, comprising: means for installing an agent on a local computer (column 4, lines 32-46, column 11, lines 40-60); means for receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 8, lines 19-31); means for decrypting the commands on the local computer utilizing the agent (column 10, lines 10-41); means for processing the commands on the local computer utilizing the agent (column 10, lines 10-41); and means for performing the risk-assessment scan on the local computer in accordance

with the processed commands to remotely detect local vulnerabilities on the local computer (column 3, lines 15-20).

Regarding claim 25, Shostack et al. teach a method of remotely detecting vulnerabilities from a remote computer, comprising: sending encrypted commands from a remote computer to an agent on a local computer for executing a risk-assessment scan utilizing a network, the commands adapted for being decrypted and processed on the local computer utilizing the agent for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 11, lines 5-67); receiving results of the risk-assessment scan from the local computer utilizing the network (column 13, lines 18-36); and transmitting feedback to the results from the remote computer to the local computer utilizing the network (column 3, lines 6-21).

Regarding claim 26, Shostack et al. teach a computer program product of remotely detecting vulnerabilities from a remote computer, comprising: computer code for sending encrypted commands from a remote computer to an agent on a local computer for executing a risk-assessment scan utilizing a network, the commands adapted for being decrypted and processed on the local computer utilizing the agent for performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 11, lines 5-67); computer code for receiving results of the risk-assessment scan from the local computer utilizing the network (column 13, lines 18-36); and computer

code for transmitting feedback to the results from the remote computer to the local computer utilizing the network (column 3, lines 6-21).

Regarding claim 27, Shostack et al. teach a method of remotely detecting vulnerabilities on a local computer, comprising: installing an agent on a local computer (column 4, lines 32-46, column 11, lines 40-60), the agent including a plurality of risk-assessment modules selected based on at least one aspect of the computer (column 2, lines 61-67, column 3, lines 1-37); receiving encrypted commands for executing a risk-assessment scan from a remote computer utilizing a network (column 8, lines 19-31); decrypting the commands on the local computer utilizing the agent (column 10, lines 10-41); authenticating the commands on the local computer utilizing the agent (column 13, lines 45-55); processing the commands on the local computer utilizing the agent, the commands adapted to execute the risk-assessment modules in a specific manner that is configured at the remote computer (column 10, lines 10-41); performing the risk-assessment scan on the local computer in accordance with the processed commands to remotely detect local vulnerabilities on the local computer (column 3, lines 15-20); transmitting results of the risk-assessment scan from the local computer to the remote computer utilizing the network (column 13, lines 18-36); receiving feedback to the results from the remote computer utilizing the network (column 3, lines 6-21).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 8, 15, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. as applied to claim 2 above, and further in view of Orchier et al.

Claims 11 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. as applied to claim 1 above, and further in view of Smid et al.

Regarding claim 4, Shostack et al. teach the limitations as set forth under claim 2 above. However, Shostack et al. do not disclose expressly the method as recited in claim 2, wherein the risk-assessment modules are selected for the agent based on specifications of the local computer.

Orchier et al. teach the method as recited in claim 2, wherein the risk-assessment modules are selected for the agent based on specifications of the local computer (column 2, lines 15-28).

Shostack et al. and Orchier et al. are analogous art because they are directed to a similar problem solving area – detecting vulnerabilities of computer systems.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to select the risk-assessment modules for the agent based on specifications of the local computer.

Therefore, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Orchier et al. with the method of Shostack et al. for the benefit of detecting computer systems vulnerabilities to obtain the invention as specified in claim 4.

Regarding claim 8, Shostack et al. teach the limitations as set forth under claim 7 above. However, Shostack et al. do not disclose expressly the method as recited in claim 7, wherein the commands are processed by extracting parameters associated with the commands, and executing the risk- assessment modules indicated by the commands utilizing the associated parameters.

Orchier et al. teach the method as recited in claim 7, wherein the commands are processed by extracting parameters associated with the commands, and executing the risk- assessment modules indicated by the commands utilizing the associated parameters (column 14, lines 25-52).

Shostack et al. and Orchier et al. are analogous art because they are directed to a similar problem solving area – detecting vulnerabilities of computer systems.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to execute the risk- assessment modules indicated by the commands utilizing the associated parameters.

Therefore, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Orchier et al. with the method of Shostack et al. for the benefit of detecting computer systems vulnerabilities to obtain the invention as specified in claim 8.

Regarding claim 15, Shostack et al. teach the limitations as set forth under claim 13 above. However, Shostack et al. do not disclose expressly the computer program product as recited in claim 13, wherein the risk- assessment modules are selected for the agent based on specifications of the local computer.

Orchier et al. teach the computer program product as recited in claim 13, wherein the risk- assessment modules are selected for the agent based on specifications of the local computer (column 2, lines 15-28).

Shostack et al. and Orchier et al. are analogous art because they are directed to a similar problem solving area – detecting vulnerabilities of computer systems.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to select the risk-assessment modules for the agent based on specifications of the local computer.

Therefore, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Orchier et al. with the method of Shostack et al. for the benefit of detecting computer systems vulnerabilities to obtain the invention as specified in claim 15.

Regarding claim 19, Shostack et al. teach the limitations as set forth under claim 18 above. However, Shostack et al. do not disclose expressly the computer program product as recited in claim 18, wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters.

Orchier et al. teach the computer program product as recited in claim 18, wherein the commands are processed by extracting parameters associated with the commands, and executing the risk-assessment modules indicated by the commands utilizing the associated parameters (column 14, lines 25-52).

Shostack et al. and Orchier et al. are analogous art because they are directed to a similar problem solving area – detecting vulnerabilities of computer systems.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to execute the risk- assessment modules indicated by the commands utilizing the associated parameters.

Therefore, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Orchier et al. with the method of Shostack et al. for the benefit of detecting computer systems vulnerabilities to obtain the invention as specified in claim 19.

Regarding claim 11, Shostack et al. teach the limitations as set forth under claim 1 above. However, Shostack et al. do not disclose expressly the method as recited in claim 1, wherein the commands are decrypted utilizing a shared key.

Smid et al. teach the method as recited in claim 1, wherein the commands are decrypted utilizing a shared key (column 3, lines 5-12).

Shostack et al. and Smid et al. are analogous art because they are directed to a similar problem solving area – encrypting commands for transfer between computer systems.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to encrypt/decrypt commands sent between computer systems over a network using a shared key.

Therefore, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Smid et al. with the method of Shostack et al. for the benefit of secure transfer of commands between computer systems to obtain the invention as specified in claim 11.

Regarding claim 22, Shostack et al. teach the limitations as set forth under claim 12 above. However, Shostack et al. do not disclose expressly the computer program product as recited in claim 12, wherein the commands are decrypted utilizing a shared key.

Smid et al. teach the computer program product as recited in claim 12, wherein the commands are decrypted utilizing a shared key (column 3, lines 5-12).

Shostack et al. and Smid et al. are analogous art because they are directed to a similar problem solving area – encrypting commands for transfer between computer systems.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to encrypt/decrypt commands sent between computer systems over a network using a shared key.

Therefore, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Smid et al. with the method of Shostack et al. for the benefit of

secure transfer of commands between computer systems to obtain the invention as specified in claim 22.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

EMMANUEL L. MOISE
PRIMARY EXAMINER
AU 2136